

CYCLIC CODES FROM THE SECOND CLASS TWO-PRIME WHITEMAN'S GENERALIZED CYCLOTOMIC SEQUENCE WITH ORDER 6

PRAMOD KUMAR KEWAT AND PRITI KUMARI

ABSTRACT. Let $n_1 = ef + 1$ and $n_2 = ef' + 1$ be two distinct odd primes with positive integers e, f, f' . In this paper, the two-prime Whiteman's generalized cyclotomic sequence of order $e = 6$ is employed to construct several classes of cyclic codes over $\text{GF}(q)$ with length $n_1 n_2$. The lower bounds on the minimum distance of these cyclic codes are obtained.

1. INTRODUCTION

Let q be a power of a prime p . An $[n, k, d]$ linear code C over a finite field $\text{GF}(q)$ is a k -dimensional subspace of the vector space $\text{GF}(q)^n$ with the minimum distance d . A linear code C is a cyclic code if the cyclic shift of a codeword in C is again a codeword in C , i.e., if $(c_0, \dots, c_{n-1}) \in C$ then $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$. Let $\gcd(n, q) = 1$. We consider the univariate polynomial ring $\text{GF}(q)[x]$ and the ideal $I = \langle x^n - 1 \rangle$ of $\text{GF}(q)[x]$. We denote by R the ring $\text{GF}(q)[x]/I$. We can consider a cyclic code of length n over $\text{GF}(q)$ as an ideal in R via the following correspondence

$$\text{GF}(q)^n \rightarrow R, \quad (c_0, c_1, \dots, c_{n-1}) \mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1}.$$

Then, a linear code C over $\text{GF}(q)$ is a cyclic code if and only if C is an ideal of R . Since R is a principal ideal ring, if C is not trivial, there exists a unique monic polynomial $g(x)$ dividing $x^n - 1$ in $\text{GF}(q)[x]$ and $C = \langle g(x) \rangle$. The polynomials $g(x)$ and $h(x) = (x^n - 1)/g(x)$ are called the generator polynomial and the parity-check polynomial of C respectively. If the dimension of the code C is k , the generator polynomial has degree $n - k$. An $[n, k, d]$ cyclic code C is capable of encoding q -ary messages of length k and requires $n - k$ redundancy symbols.

The total number of cyclic codes over $\text{GF}(q)$ and their construction are closely related to the cyclotomic cosets modulo n . One way to construct cyclic codes over $\text{GF}(q)$ with length n is to use the generator polynomial

$$\frac{x^n - 1}{\gcd(x^n - 1, S(x))}, \quad (1)$$

Key words and phrases. Cyclic codes, finite fields, cyclotomic sequences.

where $S(x) = \sum_{i=0}^{n-1} s_i x^i \in \text{GF}(q)[x]$ and $s^\infty = (s_i)_{i=0}^\infty$ is a sequence of period n over $\text{GF}(q)$. The cyclic code C_s generated by the polynomial in Eq. (1) is called the cyclic code defined by the sequence s^∞ , and the sequence s^∞ is called the defining sequence of the cyclic code C_s .

Cyclic codes have been studied in a series of papers and a lot of progress have been accomplished (see, for example [1], [6], [7], [11] and [13]). The Whiteman generalized cyclotomy was introduced by Whiteman and its properties were studied in [14]. The two-prime Whiteman's generalized cyclotomic sequence (WGCS) was introduced by Ding [4] and its coding properties were studied in [5] and [12]. Ding [5] and Sun et al. [12] constructed number of classes of cyclic codes over $\text{GF}(q)$ with length $n = n_1 n_2$ from the two-prime Whiteman's generalized cyclotomic sequences of order 2 and 4 respectively and gave the lower bounds on the minimum weight of these cyclic codes under certain conditions. Li et al. [9] gave a lower bound on linear complexity of WGCS of order six, which indicates the linear complexity is large. The autocorrelation values of WGCS were determined in [15]. Inspired by the construction of above two papers ([5] and [12]), in this paper, we employ the two-prime Whiteman's generalized cyclotomic sequences with order 6 to construct several classes of cyclic codes over $\text{GF}(q)[x]$. We also obtain lower bounds on the minimum weight of these cyclic codes.

2. PRELIMINARIES

2.1. Linear complexity and minimal polynomial. If $(s_i)_{i=0}^\infty$ is a sequence over a finite field $\text{GF}(q)$ and $f(x)$ is a polynomial with coefficients in $\text{GF}(q)$ given by

$$f(x) = c_0 + c_1 x + \cdots + c_{L-1} x^{L-1},$$

then we define

$$f(E)s_j = c_0 s_j + c_1 s_{j-1} + \cdots + c_{L-1} s_{j-L+1},$$

where E is a left shift operator defined by $Es_i = s_{i-1}$ for $i \geq 1$. Let s^n be a sequence $s_0 s_1 \cdots s_{n-1}$ of length n over a finite field $\text{GF}(q)$. For a finite sequence, the n is finite; for a semi-infinite sequence, the n is ∞ . A polynomial $f(x) \in \text{GF}(q)[x]$ of degree $\leq l$ with $c_0 \neq 0$ is called a characteristic polynomial of the sequence s^n if $f(E)s_j = 0$ for all j with $j \geq l$. For every characteristic polynomial there is a least $l \geq \deg(f)$ such that the above equation hold. The smallest l is called the associate recurrence length of $f(x)$ with respect to the sequence s^n . The characteristic polynomial with smallest length is known as minimal polynomial of the sequence s^n and the associated recurrence length is called the linear span or linear complexity of the sequence s^n .

If a semi-infinite sequence s^∞ is periodic, then its minimal polynomial is unique if $c_0 = 1$. The linear complexity of a periodic sequence is equal to the degree of its minimal polynomial. For the periodic

sequences, there are few ways to determine their linear spans and minimal polynomials. One of them is given in the following lemma.

Lemma 1. [10] *Let s^∞ be a sequence of a period n over $GF(q)$. Define*

$$S^n(x) = s_0 + s_1x + \cdots + s_{n-1}x^{n-1} \in GF(q)[x].$$

Then the minimal polynomial m_s of s^∞ is given by

$$\frac{x^n - 1}{\gcd(x^n - 1, S^n(x))}. \quad (2)$$

Consequently, the linear span L_s of s^∞ is given by

$$L_s = n - \deg(\gcd(x^n - 1, S^n(x))). \quad (3)$$

2.2. The Whiteman's generalized cyclotomic sequences and its construction. An integer a is called a primitive root of modulo n if the multiplicative order of a modulo n , denoted by $\text{ord}_n(a)$, is equal to $\phi(n)$, where $\phi(n)$ is the Euler phi function and $\gcd(a, n) = 1$.

Let n_1 and n_2 be two distinct odd primes, define $n = n_1n_2$, $d = \gcd(n_1 - 1, n_2 - 1)$ and $e = (n_1 - 1)(n_2 - 1)/d$. From the Chinese Remainder theorem, there are common primitive roots of both n_1 and n_2 . Let g be a fixed common primitive root of both n_1 and n_2 . Let u be an integer satisfying

$$u \equiv g \pmod{n_1}, \quad u \equiv 1 \pmod{n_2}. \quad (4)$$

Whiteman [14] proved that

$$\mathbb{Z}_n^* = \{g^s u^i : s = 0, 1, \dots, e-1; i = 0, 1, 2, \dots, d-1\}.$$

where \mathbb{Z}_n^* denotes the set of all invertible elements of the residue class ring \mathbb{Z}_n and e is the order of g modulo n . The Whiteman's generalized cyclotomic classes W_i of order d are defined by

$$W_i = \{g^s u^i \pmod{n} : s = 0, 1, \dots, e-1, i = 0, 1, \dots, d-1\}.$$

The classes W_i , $1 \leq i \leq d-1$ give a partition of \mathbb{Z}_n^* , i.e., $\mathbb{Z}_n^* = \cup_{i=0}^{d-1} W_i$, $W_i \cap W_j = \emptyset$ for $i \neq j$.

Let

$$P = \{n_1, 2n_1, 3n_1, \dots, (n_2 - 1)n_1\}, \quad Q = \{n_2, 2n_2, 3n_2, \dots, (n_1 - 1)n_2\},$$

$$C_0 = \{0\} \cup Q \cup \bigcup_{i=0}^{\frac{d}{2}-1} W_i, \quad C_1 = P \cup \bigcup_{i=\frac{d}{2}}^{d-1} W_i,$$

$$C_0^* = \{0\} \cup Q \cup \bigcup_{i=0}^{\frac{d}{2}-1} W_{2i} \text{ and } C_1^* = P \cup \bigcup_{i=0}^{\frac{d}{2}-1} W_{2i+1}.$$

It is easy to see that if $d > 2$, then $C_0 \neq C_0^*$ and $C_1 \neq C_1^*$. Now, we introduce two kinds of Whiteman's generalized cyclotomic sequences of order d (see [2]).

Definition. The two-prime Whiteman's generalized cyclotomic sequence $(s^*)^\infty = (s_i^*)_{i=0}^{n-1}$ of order d and period n , which is called two-prime WGCS-I, is defined by

$$s_i^* = \begin{cases} 0, & \text{if } i \in C_0^*, \\ 1, & \text{if } i \in C_1^*. \end{cases}$$

The two-prime Whiteman's generalized cyclotomic sequence $s^\infty = (s_i)_{i=0}^{n-1}$ of order d and period n , which is called two-prime WGCS-II, is defined by

$$s_i = \begin{cases} 0, & \text{if } i \in C_0, \\ 1, & \text{if } i \in C_1. \end{cases} \quad (5)$$

The cyclotomic numbers corresponding to these cyclotomic classes are defined as

$$(i, j)_d = |(W_i + 1) \cap W_j|, \text{ where } 0 \leq i, j \leq d-1.$$

Additionally, for any $t \in \mathbb{Z}_n$, we define

$$d(i, j; t) = |(W_i + t) \cap W_j|,$$

where $W_i + t = \{w + t | w \in W_i\}$.

3. A CLASS OF CYCLIC CODES OVER $\text{GF}(q)$ DEFINED BY THE TWO-PRIME WGCS

3.1. Properties of the Whiteman's cyclotomy of order d . In this subsection, we summarize number of properties of the Whiteman's generalized cyclotomy of order $d = \gcd(n_1 - 1, n_2 - 1)$. The following Lemma follows from the Theorem 4.4.6 of [3].

Lemma 2. Let the notations be same as before and $t \neq 0$. We have

$$d(i, j; t) = \begin{cases} \frac{(n_1-1)(n_2-1)}{d^2}, & i \neq j, t \in P \cup Q, \\ \frac{(n_1-1)(n_2-1-d)}{d^2}, & i = j, t \in P, t \notin Q, \\ \frac{(n_1-1-d)(n_2-1)}{d^2}, & i = j, t \in Q, t \notin P, \\ (i', j')_d \text{ for some } i', j', & \text{otherwise.} \end{cases}$$

Lemma 3. Let the symbols be defined as before. The following four statements are equivalent:

- (1) $-1 \in W_{\frac{d}{2}}$.
- (2) $\frac{(n_1-1)(n_2-1)}{d^2}$ is even.

(3) One of the following sets of equations are satisfied:

$$\begin{cases} n_1 \equiv 1 \pmod{2d} \\ n_2 \equiv d+1 \pmod{2d} \end{cases}, \quad \begin{cases} n_1 \equiv d+1 \pmod{2d} \\ n_2 \equiv 1 \pmod{2d} \end{cases}.$$

(4) $n_1 n_2 \equiv d+1 \pmod{2d}$.

Proof. (1) \Leftrightarrow (2) The result follows from (2.3) in [14].

(2) \Rightarrow (3) Let $n_1 - 1 = df$, $n_2 - 1 = df'$ and $e = df f'$, where f and f' are integer. Since $(f, f') = 1$, f and f' can not both be even. Here $f f' = \frac{(n_1-1)(n_2-1)}{d^2}$ is even. So, f or f' is even. Let f is even and f' is odd. If f is even, then $n_1 - 1 = d(2k_1)$, where k_1 is an integer. Therefore, $n_1 \equiv 1 \pmod{2d}$. If f' is odd, then $n_2 - 1 = d(2k_2 + 1)$, where k_2 is an integer. Therefore, $n_2 \equiv d+1 \pmod{2d}$. Similarly, when f is odd and f' is even. We get $n_1 \equiv d+1 \pmod{2d}$ and $n_2 \equiv 1 \pmod{2d}$.

(3) \Rightarrow (2) and (3) \Rightarrow (4) are obvious.

(4) \Rightarrow (3) Since, $\gcd(n_1 - 1, n_2 - 1) = d$, let $n_1 - 1 = fd$ and $n_2 - 1 = f'd$. We have $n_1 n_2 \equiv d+1 \pmod{2d}$, this gives $fd + f'd \equiv d \pmod{2d}$. Thus, we have $f + f' = 2k + 1$ for an integer k . So, $n_1 = 2kd + (1 - f')d + 1$, this gives $n_1 \equiv (1 - f')d + 1 \pmod{2d}$. If f' is odd, then $n_1 \equiv 1 \pmod{2d}$ and $n_2 \equiv d+1 \pmod{2d}$. If f' is even, then $n_1 \equiv d+1 \pmod{2d}$ and $n_2 \equiv 1 \pmod{2d}$. \square

Lemma 4. *Let the symbols be defined as before. The following four statements are equivalent:*

(1) $-1 \in W_0$.

(2) $\frac{(n_1-1)(n_2-1)}{d^2}$ is odd.

(3) The following set of equation is satisfied:

$$\begin{cases} n_1 \equiv d+1 \pmod{2d} \\ n_2 \equiv d+1 \pmod{2d} \end{cases},$$

(4) $n_1 n_2 \equiv 1 \pmod{2d}$.

Proof. Similar to the proof of the above lemma. \square

3.2. Properties of Whiteman's cyclotomy of order 6. We recall the following lemmas (Lemma 1 and Lemma 2) from [8].

Lemma 5. *Let $\gcd(n_1 - 1, n_2 - 1) = 6$, i.e., $n_1 \equiv 1 \pmod{6}$, $n_2 \equiv 1 \pmod{6}$. Let a, b, x, y, c and d are integers. There are 10 possible different cyclotomic numbers of order 6 and they are given by the following relations:*

If $\frac{(n_1-1)(n_2-1)}{36}$ is odd, we have

$$\begin{aligned}
(0,0)_6 &= \frac{1}{72}(12M + 32 + 6a - 24x + 2c), \\
(0,1)_6 &= (1,0)_6 = (5,5)_6 = \frac{1}{72}(12M + 8 + a + 3b + 8x + 24y - c + 9d), \\
(0,2)_6 &= (2,0)_6 = (4,4)_6 = \frac{1}{72}(12M + 8 - 3a + 9b - c - 9d), \\
(0,3)_6 &= (3,0)_6 = (3,3)_6 = \frac{1}{72}(12M + 8 - 2a + 8x + 2c), \\
(0,4)_6 &= (4,0)_6 = (2,2)_6 = \frac{1}{72}(12M + 8 - 3a - c - 9b + 9d), \\
(0,5)_6 &= (5,0)_6 = (1,1)_6 = \frac{1}{72}(12M + 8 + a - 3b + 8x - 24y - c - 9d), \\
(1,2)_6 &= (2,1)_6 = (4,5)_6 = (5,4)_6 = (5,1)_6 = (1,5)_6 = \frac{1}{72}(12M - 4 - 2a - 4x + 2c), \\
(1,3)_6 &= (2,5)_6 = (3,1)_6 = (3,4)_6 = (4,3)_6 = (5,2)_6 = \frac{1}{72}(12M - 4 + a + 3b - 4x - 12y - c + 9d), \\
(1,4)_6 &= (2,3)_6 = (3,2)_6 = (3,5)_6 = (4,1)_6 = (5,3)_6 = \frac{1}{72}(12M - 4 + a - 3b - 4x + 12y - c - 9d) \text{ and} \\
(2,4)_6 &= (4,2)_6 = \frac{1}{72}(12M - 4 + 6a + 12x + 2c).
\end{aligned}$$

If $\frac{(n_1-1)(n_2-1)}{36}$ is even, we have

$$\begin{aligned}
(0,0)_6 &= (3,0)_6 = (3,3)_6 = \frac{1}{72}(12M + 20 - 8x - 2a + 2c), \\
(0,1)_6 &= (2,5)_6 = (4,3)_6 = \frac{1}{72}(12M - 4 - 3a - 9b - c + 9d), \\
(0,2)_6 &= (1,4)_6 = (5,3)_6 = \frac{1}{72}(12M - 4 - 8x + a - c + 24y - 3b - 9d), \\
(0,3)_6 &= \frac{1}{72}(12M - 4 + 24x + 6a + 2c), \\
(0,4)_6 &= (1,3)_6 = (5,2)_6 = \frac{1}{72}(12M - 4 - 8x + a - c - 24y + 3b + 9d), \\
(0,5)_6 &= (2,3)_6 = (4,1)_6 = \frac{1}{72}(12M - 4 - 3a - c + 9b - 9d), \\
(1,0)_6 &= (2,2)_6 = (3,1)_6 = (3,4)_6 = (4,0)_6 = (5,5)_6 = \frac{1}{72}(12M + 8 + 4x + a - c + 12y + 3b + 9d), \\
(1,1)_6 &= (2,0)_6 = (3,2)_6 = (3,5)_6 = (4,4)_6 = (5,0)_6 = \frac{1}{72}(12M + 8 + 4x + a - c - 12y - 3b - 9d), \\
(1,2)_6 &= (1,5)_6 = (2,4)_6 = (4,2)_6 = (5,1)_6 = (5,4)_6 = \frac{1}{72}(12M - 4 + 4x - 2a + 2c) \text{ and} \\
(2,1)_6 &= (4,5)_6 = \frac{1}{72}(12M - 4 + 6a - 12x + 2c).
\end{aligned}$$

Where $n_1 n_2 = x^2 + 3y^2$, $M = \frac{1}{6}((n_1 - 2)(n_2 - 2) - 1)$ and $4n_1 n_2 = a^2 + 3b^2 = c^2 + 27d^2$.

From [[3], Theorem I.15 and page 118], we get following relation between the parameters a, b, x, y, c and d .

Lemma 6. Let k and l be integer such that $k \equiv g \pmod{(n_1)}$ and $l \equiv g \pmod{(n_2)}$. Suppose $k^\rho = 2 \in \mathbb{F}_{n_1}$ and $l^\varrho = 2 \in \mathbb{F}_{n_2}$ for some integers ρ and ϱ . Let the parameters a, b, x, y, c, d be same as in the above lemma. Then, we have the following results.

Case-I If $\{(n_1 - 1)(n_2 - 1)\}/36$ is even, we have

- 1) If $\rho - \varrho \equiv 0 \pmod{3}$, then $a = 2x = -c$, $b = -2y = -3d$.
- 2) If $\rho - \varrho \equiv 1 \pmod{3}$, then $a = -x - 3y$, $b = -x + y$, $c = x - 3y$, $3d = -x - y$.
- 3) If $\rho - \varrho \equiv 2 \pmod{3}$, then $a = -x + 3y$, $b = x + y$, $c = x + 3y$, $3d = x - y$.

Case-II $\{(n_1 - 1)(n_2 - 1)\}/36$ is odd, we have

- 1) If $\rho - \varrho \equiv 0 \pmod{3}$, then $a = -2x = c$, $b = 2y = 3d$.
- 2) If $\rho - \varrho \equiv 1 \pmod{3}$, then $a = x + 3y$, $b = x - y$, $c = x - 3y$, $3d = -x - y$.
- 3) If $\rho - \varrho \equiv 2 \pmod{3}$, then $a = x - 3y$, $b = -x - y$, $c = x + 3y$, $3d = x - y$.

Furthermore, we get the following form for the cyclotomic numbers of order 6 after substituting the value of a, b, c and d from Lemma 6 to Lemma 5.

TABLE 1. The cyclotomic number of order 6 for even $\{(n_1 - 1)(n_2 - 1)\}/36$

	$\rho - \varrho \equiv 0 \pmod{3}$	$\rho - \varrho \equiv 1 \pmod{3}$	$\rho - \varrho \equiv 2 \pmod{3}$
$36(0, 0)_6$	$6M + 10 - 8x$	$6M + 10 - 2x$	$6M + 10 - 2x$
$36(0, 1)_6$	$6M - 2 - 2x + 12y$	$6M - 2 + 4x$	$6M - 2 - 2x - 12y$
$36(0, 2)_6$	$6M - 2 - 2x + 12y$	$6M - 2 - 2x + 12y$	$6M - 2 - 8x + 12y$
$36(0, 3)_6$	$6M - 2 + 16x$	$6M - 2 + 10x - 12y$	$6M - 2 + 10x + 12y$
$36(0, 4)_6$	$6M - 2 - 2x - 12y$	$6M - 2 - 8x - 12y$	$6M - 2 - 2x - 12y$
$36(0, 5)_6$	$6M - 2 - 2x - 12y$	$6M - 2 - 2x + 12y$	$6M - 2 + 4x$
$36(1, 0)_6$	$6M + 4 + 4x + 6y$	$6M + 4 - 2x + 6y$	$6M + 4 + 4x + 6y$
$36(1, 1)_6$	$6M + 4 + 4x - 6y$	$6M + 4 + 4x - 6y$	$6M + 4 - 2x - 6y$
$36(1, 2)_6$	$6M - 2 - 2x$	$6M - 2 + 4x$	$6M - 2 + 4x$
$36(2, 1)_6$	$6M - 2 - 2x$	$6M - 2 - 8x - 12y$	$6M - 2 - 8x + 12y$

TABLE 2. The cyclotomic number of order 6 for odd $\{(n_1 - 1)(n_2 - 1)\}/36$

	$\rho - \varrho \equiv 0 \pmod{3}$	$\rho - \varrho \equiv 1 \pmod{3}$	$\rho - \varrho \equiv 2 \pmod{3}$
$36(0, 0)_6$	$6M + 16 - 20x$	$6M + 16 - 8x + 6y$	$6M + 16 - 8x - 6y$
$36(0, 1)_6$	$6M + 4 + 4x + 18y$	$6M + 4 + 4x + 12y$	$6M + 4 + 4x + 6y$
$36(0, 2)_6$	$6M + 4 + 4x + 6y$	$6M + 4 + 4x - 6y$	$6M + 4 - 8x$
$36(0, 3)_6$	$6M + 4 + 4x$	$6M + 4 + 4x - 6y$	$6M + 4 + 4x + 6y$
$36(0, 4)_6$	$6M + 4 + 4x - 6y$	$6M + 4 - 8x$	$6M + 4 + 4x + 6y$
$36(0, 5)_6$	$6M + 4 + 4x - 18y$	$6M + 4 + 4x - 6y$	$6M + 4 + 4x - 12y$
$36(1, 2)_6$	$6M - 2 - 2x$	$6M - 2 - 2x - 6y$	$6M - 2 - 2x + 6y$
$36(1, 3)_6$	$6M - 2 - 2x$	$6M - 2 - 2x - 6y$	$6M - 2 - 2x - 12y$
$36(1, 4)_6$	$6M - 2 - 2x$	$6M - 2 - 2x + 12y$	$6M - 2 - 2x + 6y$
$36(2, 4)_6$	$6M - 2 - 2x$	$6M - 2 + 10x + 6y$	$6M - 2 + 10x - 6y$

These 36 cyclotomic numbers (i, j) are solely functions of the unique representation of $p = x^2 + 3y^2$; $x \equiv 1 \pmod{3}$ and the sign of y is ambiguously determined.

Lemma 7. [14] Define $\eta = \frac{(n_1-1)(n_2-1)}{36}$. Let symbols be same as before. Then

$$-1 \in \begin{cases} W_0, & \text{if } \eta \text{ is odd,} \\ W_3, & \text{if } \eta \text{ is even.} \end{cases}$$

3.3. A class of cyclic codes over $\text{GF}(q)$ defined by two-prime WGCS-II. We have $\gcd(n, q) = 1$. Let m be the order of q modulo n . Then the field $\text{GF}(q^m)$ has a primitive n th root of unity β . We define

$$S(x) = \sum_{i \in C_1} x^i = \left(\sum_{i \in P} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) x^i \in \text{GF}(q)[x], \quad (6)$$

$$T(x) = \left(\sum_{i \in P} + \sum_{i \in W_1} + \sum_{i \in W_2} + \sum_{i \in W_3} \right) x^i \in \text{GF}(q)[x] \text{ and} \quad (7)$$

$$U(x) = \left(\sum_{i \in P} + \sum_{i \in W_2} + \sum_{i \in W_3} + \sum_{i \in W_4} \right) x^i \in \text{GF}(q)[x]. \quad (8)$$

Our main aim in this section is to find the generator polynomial

$$g(x) = \frac{x^n - 1}{\gcd(x^n - 1, S(x))}.$$

of the cyclic code C_s defined by the sequence s^∞ . To compute the parameters of the cyclic code C_s defined by the sequence s^∞ , we need to compute $\gcd(x^n - 1, S(x))$. Since β is a primitive n th root of unity, we need only to find such t 's that $S(\beta^t) = 0$, where $0 \leq t \leq n - 1$. To this end, we need number of auxiliary results. We have

$$0 = \beta^n - 1 = (\beta^{n_1})^{n_2} - 1 = (\beta^{n_1} - 1)(1 + \beta^{n_1} + \beta^{2n_1} + \dots + \beta^{(n_2-1)n_1}).$$

It follows that

$$\beta^{n_1} + \beta^{2n_1} + \dots + \beta^{(n_2-1)n_1} = -1, \text{ i.e., } \sum_{i \in P} \beta^i = -1. \quad (9)$$

By symmetry we get

$$\beta^{n_2} + \beta^{2n_2} + \dots + \beta^{(n_1-1)n_2} = -1, \text{ i.e., } \sum_{i \in Q} \beta^i = -1. \quad (10)$$

Lemma 8. Let the symbols be same as before. For $0 \leq j \leq 5$, we have

$$\sum_{i \in W_j} \beta^{it} = \begin{cases} -\frac{n_1-1}{6} \pmod{p}, & \text{if } t \in P, \\ -\frac{n_2-1}{6} \pmod{p}, & \text{if } t \in Q. \end{cases}$$

Proof. Suppose that $t \in Q$. Since g is a common primitive roots of n_1 and n_2 and the order of g modulo n is e , by the definition of u , we have

$$\begin{aligned} W_j \bmod n_1 &= \{g^s u^j \bmod n_1 : s = 0, 1, 2, \dots, e-1\} \\ &= \{g^{s+j} \bmod n_1 : s = 0, 1, 2, \dots, e-1\} \\ &= \frac{n_2-1}{6} * \{1, 2, \dots, n_1-1\}, \end{aligned}$$

where $\frac{n_2-1}{6}$ denotes the multiplicity of each element in the set $\{1, 2, \dots, n_1-1\}$. We can write $g^s x^j$ in the form

$$\begin{aligned} &1 + k_{11}n_1, 1 + k_{12}n_1, \dots, 1 + k_{1(n_2-1)/6}n_1, \\ &2 + k_{21}n_1, 2 + k_{22}n_1, \dots, 2 + k_{2(n_2-1)/6}n_1, \\ &\vdots \\ &n_1 - 1 + k_{(n_1-1)1}n_1, n_1 - 1 + k_{(n_1-1)2}n_1, \dots, n_1 - 1 + k_{(n_1-1)(n_2-1)/6}n_1. \end{aligned} \quad (11)$$

where k_{li} is an positive integer, $1 \leq l \leq n_1 - 1$ and $1 \leq i \leq (n_2 - 1)/6$.

When s ranges over $\{0, 1, \dots, e-1\}$, we divides the set W_j into $(n_2-1)/6$ subsets each of which contains $n_1 - 1$ consecutive integers, i.e., $g^{s+j} \bmod n_1$ takes on each element of $\{1, 2, \dots, n_1-1\}$ exactly $\frac{n_2-1}{6}$ times. From (11), it follows that if $t \in Q$, we have $\beta^{(m+k_{li}n_1)t} = \beta^{mt}$, where $1 \leq m \leq n_1 - 1$. It follows from (10) that

$$\sum_{i \in W_j} \beta^{it} = \left(\frac{n_2-1}{6}\right) \sum_{j \in Q} \beta^j = -\frac{n_2-1}{6} \pmod{p}.$$

For $t \in P$, we can get the result by similar argument. \square

Lemma 9. For any $r \in W_i$, we have $rW_j = W_{i+j \pmod{d}}$, where $rW_j = \{rt \mid t \in W_j\}$.

Proof. We have $W_i = \{g^s u^i : s = 0, 1, 2, \dots, e-1\}$, $i = 0, 1, \dots, d-1$ and let $r = g^{s_1} u^i \in W_i$. Then $rW_j = g^{s_1} u^i \{u^j + gu^j + g^1 u^j + \dots + g^{e-1} u^j\} = \{g^{s_1} u^{i+j} + g^{s_1+1} u^{i+j} + \dots + g^{s_1+e-1} u^{i+j}\}$. Since $u \in \mathbb{Z}_n^*$, there must exist an integer v with $0 \leq v \leq e-1$ such that $u^d = g^v$, therefore, we must have $rW_j = W_{i+j \pmod{d}}$. \square

Lemma 10. *For all $t \in \mathbb{Z}_n$, we have*

$$S(\beta^t) = \begin{cases} -\frac{n_1+1}{2} \pmod{p}, & \text{if } t \in P, \\ \frac{n_2-1}{2} \pmod{p}, & \text{if } t \in Q, \\ S(\beta), & \text{if } t \in W_0, \\ -(T(\beta) + 1), & \text{if } t \in W_1, \\ -(U(\beta) + 1), & \text{if } t \in W_2, \\ -(S(\beta) + 1), & \text{if } t \in W_3, \\ T(\beta), & \text{if } t \in W_4, \\ U(\beta), & \text{if } t \in W_5, \end{cases}$$

$$T(\beta^t) = \begin{cases} -\frac{n_1+1}{2} \pmod{p}, & \text{if } t \in P, \\ \frac{n_2-1}{2} \pmod{p}, & \text{if } t \in Q, \\ T(\beta), & \text{if } t \in W_0, \\ U(\beta), & \text{if } t \in W_1, \\ S(\beta), & \text{if } t \in W_2, \\ -(T(\beta) + 1), & \text{if } t \in W_3, \\ -(U(\beta) + 1), & \text{if } t \in W_4, \\ -(S(\beta) + 1), & \text{if } t \in W_5, \end{cases}$$

and

$$U(\beta^t) = \begin{cases} -\frac{n_1+1}{2} \pmod{p}, & \text{if } t \in P, \\ \frac{n_2-1}{2} \pmod{p}, & \text{if } t \in Q, \\ U(\beta), & \text{if } t \in W_0, \\ S(\beta), & \text{if } t \in W_1, \\ -(T(\beta) + 1), & \text{if } t \in W_2, \\ -(U(\beta) + 1), & \text{if } t \in W_3, \\ -(S(\beta) + 1), & \text{if } t \in W_4, \\ T(\beta), & \text{if } t \in W_5. \end{cases}$$

Proof. Since $\gcd(n_1, n_2) = 1$, if $t \in P$ then $tP = P$. Then by (9) and Lemma 8, we get

$$\begin{aligned} S(\beta^t) &= \sum_{i \in C_1} \beta^{ti} = \left(\sum_{i \in P} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^{ti} \\ &= (-1 \pmod{p}) - \left(\frac{n_1-1}{6} \pmod{p} \right) - \left(\frac{n_1-1}{6} \pmod{p} \right) - \left(\frac{n_1-1}{6} \pmod{p} \right) \\ &= -\frac{n_1+1}{2} \pmod{p}. \end{aligned}$$

If $t \in Q$, then $tP = 0$. Then by (9) and Lemma 8, we get

$$\begin{aligned}
 S(\beta^t) &= \sum_{i \in C_1} \beta^{ti} = \left(\sum_{i \in P} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^{ti} \\
 &= (n_2 - 1 \bmod p) - \left(\frac{n_2 - 1}{6} \bmod p \right) - \left(\frac{n_2 - 1}{6} \bmod p \right) - \left(\frac{n_2 - 1}{6} \bmod p \right) \\
 &= \frac{n_2 - 1}{2} \bmod p.
 \end{aligned}$$

By Lemma 9, $tW_i = W_i$ if $t \in W_0$. If $t \in W_0$, then $tP = P$ since $\gcd(t, n_2) = 1$. Hence

$$\begin{aligned}
 S(\beta^t) &= \sum_{i \in C_1} \beta^{ti} = \left(\sum_{i \in P} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^{ti} \\
 &= \left(\sum_{i \in P} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i \\
 &= S(\beta).
 \end{aligned}$$

By Lemma 9, if $t \in W_1$ then $tW_i = W_{(i+1) \bmod 6}$ for $0 \leq i \leq 5$. And since $\gcd(a, n_2) = 1$, if $t \in W_1$

then $tP = P$. We have $\beta^n - 1 = (\beta - 1) \left(\sum_{i=0}^{n-1} \beta^i \right) = 0$ and $\beta - 1 \neq 0$, this gives $\sum_{i=0}^{n-1} \beta^i = 0$. Therefore,

$$\sum_{i=0}^{n-1} \beta^i = 1 + \sum_{i \in P} \beta^i + \sum_{i \in Q} \beta^i + \sum_{i \in \bigcup_{j=0}^5 W_j} \beta^i = 0.$$

From (9) and (10), we get

$$\sum_{i \in \bigcup_{j=0}^5 W_j} \beta^i = 1. \tag{12}$$

Hence

$$\begin{aligned}
S(\beta^t) &= \sum_{i \in C_1} \beta^{ti} = \left(\sum_{i \in P} + \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^{ti} \\
&= \left(\sum_{i \in P} + \sum_{i \in W_4} + \sum_{i \in W_5} + \sum_{i \in W_0} \right) \beta^i \\
&= \left(\sum_{i \in P} - \sum_{i \in W_1} - \sum_{i \in W_2} - \sum_{i \in W_3} \right) \beta^i + 1 \\
&= \left(-\sum_{i \in P} - \sum_{i \in W_1} - \sum_{i \in W_2} - \sum_{i \in W_3} \right) \beta^i + 2 \sum_{i \in P} \beta^i + 1 \\
&= -(T(\beta) + 1).
\end{aligned}$$

Similarly, we can get the result when $t \in W_i$, $2 \leq i \leq 5$.

In a similar fashion, we can get the result for $T(\beta^t)$ and $U(\beta^t)$. This completes the proof of this lemma. \square

Note that

$$S(1) = \frac{(n_1 + 1)(n_2 - 1)}{2} \pmod{p}. \quad (13)$$

Corollary 1. *Let the symbols be defined as before. We have the following conclusions.*

- (I) If $q \notin W_0$, we have $S(\beta) \neq 0, -1$, $T(\beta) \neq 0, -1$ and $U(\beta) \neq 0, -1$.
- (II) If $q \in W_0$, we have $S^q(\beta) = S(\beta)$, $T^q(\beta) = T(\beta)$ and $U^q(\beta) = U(\beta)$ and $S(\beta), T(\beta), U(\beta) \in GF(q)$.

Proof. (I) Note that $\gcd(n, q) = 1$, i.e., $q \in \mathbb{Z}_n^*$ then $q \in \bigcup_{i=1}^5 W_i$. If $q \notin W_0$, without loss of generality, assume that $q \in W_1$. By Lemma 10, we have

$$S^{q^3}(\beta) = S^{q^2}(\beta^q) = (-T(\beta) - 1)^{q^2} = (-T(\beta^q) - 1)^q = (-U(\beta) - 1)^q = (-U(\beta^q) - 1) = -S(\beta) - 1,$$

i.e.,

$$S^{q^3}(\beta) + S(\beta) + 1 = 0. \quad (14)$$

It is easy to see that 0 and -1 is not the solution of Eq. (14). Similarly, we have

$$T^{q^3}(\beta) + T(\beta) + 1 = 0,$$

and

$$U^{q^3}(\beta) + U(\beta) + 1 = 0,$$

i.e., $T(\beta) \neq 0, -1$ and $U(\beta) \neq 0, -1$. If $q \in W_i, 2 \leq i \leq 5$ the results can be proved by similar argument.

(II) If $q \in W_0$, the conclusion is obvious. \square

Lemma 11. *Let the symbols be the same as before. We have the following conclusions.*

(I) If η is odd, then we have three cases:

Case (A) If $\rho - \varrho \equiv 0 \pmod{3}$,

$$\begin{aligned} S(\beta)(S(\beta) + 1) &= \frac{n-1}{4} - \frac{2y}{3} \left(-\sum_{i \in W_0} + \sum_{i \in W_2} - \sum_{i \in W_3} + \sum_{i \in W_5} \right) \beta^i, \\ T(\beta)(T(\beta) + 1) &= \frac{n-1}{4} - \frac{2y}{3} \left(\sum_{i \in W_0} - \sum_{i \in W_1} + \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i \text{ and} \\ U(\beta)(U(\beta) + 1) &= \frac{n-1}{4} - \frac{2y}{3} \left(\sum_{i \in W_1} - \sum_{i \in W_2} + \sum_{i \in W_4} - \sum_{i \in W_5} \right) \beta^i. \end{aligned}$$

Case (B) If $\rho - \varrho \equiv 1 \pmod{3}$,

$$\begin{aligned} S(\beta)(S(\beta) + 1) &= \frac{n-1}{4} + \frac{x+y}{3} \left(\sum_{i \in W_1} - \sum_{i \in W_2} + \sum_{i \in W_4} - \sum_{i \in W_5} \right) \beta^i, \\ T(\beta)(T(\beta) + 1) &= \frac{n-1}{4} + \frac{x+y}{3} \left(-\sum_{i \in W_0} + \sum_{i \in W_2} - \sum_{i \in W_3} + \sum_{i \in W_5} \right) \beta^i \text{ and} \\ U(\beta)(U(\beta) + 1) &= \frac{n-1}{4} + \frac{x+y}{3} \left(\sum_{i \in W_0} - \sum_{i \in W_1} + \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i. \end{aligned}$$

Case (C) If $\rho - \varrho \equiv 2 \pmod{3}$,

$$\begin{aligned} S(\beta)(S(\beta) + 1) &= \frac{n-1}{4} - \frac{x-y}{3} \left(\sum_{i \in W_0} - \sum_{i \in W_1} + \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i, \\ T(\beta)(T(\beta) + 1) &= \frac{n-1}{4} - \frac{x-y}{3} \left(\sum_{i \in W_1} - \sum_{i \in W_2} + \sum_{i \in W_4} - \sum_{i \in W_5} \right) \beta^i \text{ and} \\ U(\beta)(U(\beta) + 1) &= \frac{n-1}{4} - \frac{x-y}{3} \left(-\sum_{i \in W_0} + \sum_{i \in W_2} - \sum_{i \in W_3} + \sum_{i \in W_5} \right) \beta^i. \end{aligned}$$

(II) If η is even, then we have three cases:

Case (A) If $\rho - \varrho \equiv 0 \pmod{3}$,

$$\begin{aligned} S(\beta)(S(\beta) + 1) &= -\frac{n+1}{4} + \frac{2y}{3} \left(-\sum_{i \in W_0} + \sum_{i \in W_2} - \sum_{i \in W_3} + \sum_{i \in W_5} \right) \beta^i, \\ T(\beta)(T(\beta) + 1) &= -\frac{n+1}{4} + \frac{2y}{3} \left(\sum_{i \in W_0} - \sum_{i \in W_1} + \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i \text{ and} \\ U(\beta)(U(\beta) + 1) &= -\frac{n+1}{4} + \frac{2y}{3} \left(\sum_{i \in W_1} - \sum_{i \in W_2} + \sum_{i \in W_4} - \sum_{i \in W_5} \right) \beta^i. \end{aligned}$$

Case (B) If $\rho - \varrho \equiv 1 \pmod{3}$,

$$\begin{aligned} S(\beta)(S(\beta) + 1) &= -\frac{n+1}{4} - \frac{x+y}{3} \left(\sum_{i \in W_1} - \sum_{i \in W_2} + \sum_{i \in W_4} - \sum_{i \in W_5} \right) \beta^i, \\ T(\beta)(T(\beta) + 1) &= -\frac{n+1}{4} - \frac{x+y}{3} \left(-\sum_{i \in W_0} + \sum_{i \in W_2} - \sum_{i \in W_3} + \sum_{i \in W_5} \right) \beta^i \text{ and} \\ U(\beta)(U(\beta) + 1) &= -\frac{n+1}{4} - \frac{x+y}{3} \left(\sum_{i \in W_0} - \sum_{i \in W_1} + \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i. \end{aligned}$$

Case (C) If $\rho - \varrho \equiv 2 \pmod{3}$,

$$\begin{aligned} S(\beta)(S(\beta) + 1) &= -\frac{n+1}{4} + \frac{x-y}{3} \left(\sum_{i \in W_0} - \sum_{i \in W_1} + \sum_{i \in W_3} - \sum_{i \in W_4} \right) \beta^i, \\ T(\beta)(T(\beta) + 1) &= -\frac{n+1}{4} + \frac{x-y}{3} \left(\sum_{i \in W_1} - \sum_{i \in W_2} + \sum_{i \in W_4} - \sum_{i \in W_5} \right) \beta^i \text{ and} \\ U(\beta)(U(\beta) + 1) &= -\frac{n+1}{4} + \frac{x-y}{3} \left(-\sum_{i \in W_0} + \sum_{i \in W_2} - \sum_{i \in W_3} + \sum_{i \in W_5} \right) \beta^i. \end{aligned}$$

Proof. (I) By the definition of $S(x)$ and from (9), we have

$$S(\beta) = -1 + \left(\sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i.$$

Then, we get

$$\begin{aligned}
S(\beta)(S(\beta+1)) = & - \left(\sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i + \left(\sum_{i \in W_3} \sum_{j \in W_3} + \sum_{i \in W_4} \sum_{j \in W_4} + \sum_{i \in W_5} \sum_{j \in W_5} \right) \beta^{i+j} \\
& + \left(2 \sum_{i \in W_3} \sum_{j \in W_4} + 2 \sum_{i \in W_3} \sum_{j \in W_5} + 2 \sum_{i \in W_4} \sum_{j \in W_5} \right) \beta^{i+j}.
\end{aligned} \tag{15}$$

From Lemma 7, if η is odd then $-1 \in W_0$ and that $-W_j = \{-t : t \in W_j\} = W_j$.

$$\begin{aligned}
\sum_{i \in W_3} \sum_{j \in W_3} \beta^{i+j} &= \sum_{i \in W_3} \sum_{j \in W_3} \beta^{i-j} \\
&= |W_3| + \sum_{r \in P \cup Q} d(3, 3; r) \beta^r + (3, 3)_6 \sum_{i \in W_0} \beta^i + (2, 2)_6 \sum_{i \in W_1} \beta^i + (1, 1)_6 \sum_{i \in W_2} \beta^i + (0, 0)_6 \sum_{i \in W_3} \beta^i \\
&\quad + (5, 5)_6 \sum_{i \in W_4} \beta^i + (4, 4)_6 \sum_{i \in W_5} \beta^i,
\end{aligned} \tag{16}$$

$$\begin{aligned}
\sum_{i \in W_4} \sum_{j \in W_4} \beta^{i+j} &= \sum_{i \in W_4} \sum_{j \in W_4} \beta^{i-j} \\
&= |W_4| + \sum_{r \in P \cup Q} d(4, 4; r) \beta^r + (4, 4)_6 \sum_{i \in W_0} \beta^i + (3, 3)_6 \sum_{i \in W_1} \beta^i + (2, 2)_6 \sum_{i \in W_2} \beta^i + (1, 1)_6 \sum_{i \in W_3} \beta^i \\
&\quad + (0, 0)_6 \sum_{i \in W_4} \beta^i + (5, 5)_6 \sum_{i \in W_5} \beta^i,
\end{aligned} \tag{17}$$

$$\begin{aligned}
\sum_{i \in W_5} \sum_{j \in W_5} \beta^{i+j} &= \sum_{i \in W_5} \sum_{j \in W_5} \beta^{i-j} \\
&= |W_5| + \sum_{r \in P \cup Q} d(5, 5; r) \beta^r + (5, 5)_6 \sum_{i \in W_0} \beta^i + (4, 4)_6 \sum_{i \in W_1} \beta^i + (3, 3)_6 \sum_{i \in W_2} \beta^i + (2, 2)_6 \sum_{i \in W_3} \beta^i \\
&\quad + (1, 1)_6 \sum_{i \in W_4} \beta^i + (0, 0)_6 \sum_{i \in W_5} \beta^i,
\end{aligned} \tag{18}$$

$$\begin{aligned}
2 \sum_{i \in W_3} \sum_{j \in W_4} \beta^{i+j} &= \sum_{i \in W_3} \sum_{j \in W_4} \beta^{i-j} \\
&= 2 \left(\sum_{r \in P \cup Q} d(4, 3; r) \beta^r + (4, 3)_6 \sum_{i \in W_0} \beta^i + (3, 2)_6 \sum_{i \in W_1} \beta^i + (2, 1)_6 \sum_{i \in W_2} \beta^i + (1, 0)_6 \sum_{i \in W_3} \beta^i \right. \\
&\quad \left. + (0, 5)_6 \sum_{i \in W_4} \beta^i + (5, 4)_6 \sum_{i \in W_5} \beta^i \right),
\end{aligned} \tag{19}$$

$$\begin{aligned}
2 \sum_{i \in W_3} \sum_{j \in W_5} \beta^{i+j} &= \sum_{i \in W_3} \sum_{j \in W_5} \beta^{i-j} \\
&= 2 \left(\sum_{r \in P \cup Q} d(5, 3; r) \beta^r + (5, 3)_6 \sum_{i \in W_0} \beta^i + (4, 2)_6 \sum_{i \in W_1} \beta^i + (3, 1)_6 \sum_{i \in W_2} \beta^i + (2, 0)_6 \sum_{i \in W_3} \beta^i \right. \\
&\quad \left. + (1, 5)_6 \sum_{i \in W_4} \beta^i + (0, 4)_6 \sum_{i \in W_5} \beta^i \right), \tag{20}
\end{aligned}$$

$$\begin{aligned}
2 \sum_{i \in W_4} \sum_{j \in W_5} \beta^{i+j} &= \sum_{i \in W_4} \sum_{j \in W_5} \beta^{i-j} \\
&= 2 \left(\sum_{r \in P \cup Q} d(5, 4; r) \beta^r + (5, 4)_6 \sum_{i \in W_0} \beta^i + (4, 3)_6 \sum_{i \in W_1} \beta^i + (3, 2)_6 \sum_{i \in W_2} \beta^i + (2, 1)_6 \sum_{i \in W_3} \beta^i \right. \\
&\quad \left. + (1, 0)_6 \sum_{i \in W_4} \beta^i + (0, 5)_6 \sum_{i \in W_5} \beta^i \right), \tag{21}
\end{aligned}$$

Substituting (16 - 21) into (15) and combining Lemma 2, Lemma 5 and (12), we get

$$\begin{aligned}
S(\beta)(S(\beta) + 1) &= - \left(\sum_{i \in W_3} \beta^i + \sum_{i \in W_4} \beta^i + \sum_{i \in W_5} \beta^i \right) + \left(\frac{3M}{2} - \frac{8x - 4a}{72} + \frac{12b + 24y}{72} \right) \sum_{i \in W_0} \beta^i \\
&\quad + \left(\frac{3M}{2} - \frac{16x + 8a}{72} \right) \sum_{i \in W_1} \beta^i + \left(\frac{3M}{2} - \frac{8x - 4a}{72} - \frac{12b + 24y}{72} \right) \sum_{i \in W_2} \beta^i \\
&\quad + \left(\frac{3M}{2} + 1 - \frac{8x - 4a}{72} + \frac{12b + 24y}{72} \right) \sum_{i \in W_3} \beta^i + \left(\frac{3M}{2} + 1 + \frac{16x + 8a}{72} \right) \sum_{i \in W_4} \beta^i \\
&\quad + \left(\frac{3M}{2} + 1 - \frac{8x - 4a}{72} - \frac{24y - 12b}{72} \right) \sum_{i \in W_5} \beta^i - 12 \frac{(n_1 - 1)(n_2 - 1)}{36} - 3 \frac{(n_1 - 1)(n_2 - 7)}{36} \\
&\quad - 3 \frac{(n_1 - 7)(n_2 - 1)}{36} + 3 \frac{(n_1 - 1)(n_2 - 1)}{6} \\
&= \frac{n - 1}{4} - \frac{a + 2x}{18} \left(\sum_{i \in W_0} -2 \sum_{i \in W_1} + \sum_{i \in W_2} + \sum_{i \in W_3} -2 \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i \\
&\quad + \frac{b + 2y}{6} \left(\sum_{i \in W_0} - \sum_{i \in W_2} + \sum_{i \in W_3} - \sum_{i \in W_5} \right) \beta^i.
\end{aligned}$$

By the same argument as above, we can get

$$T(\beta)(T(\beta) + 1) = \frac{n-1}{4} - \frac{a+2x}{18} \left(\sum_{i \in W_0} + \sum_{i \in W_1} - 2 \sum_{i \in W_2} + \sum_{i \in W_3} + \sum_{i \in W_4} - 2 \sum_{i \in W_5} \right) \beta^i$$

$$+ \frac{b+2y}{6} \left(- \sum_{i \in W_0} + \sum_{i \in W_1} - \sum_{i \in W_3} + \sum_{i \in W_4} \right) \beta^i \text{ and}$$

$$U(\beta)(U(\beta) + 1) = \frac{n-1}{4} - \frac{a+2x}{18} \left(-2 \sum_{i \in W_0} + \sum_{i \in W_1} + \sum_{i \in W_2} - 2 \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i$$

$$+ \frac{b+2y}{6} \left(- \sum_{i \in W_1} + \sum_{i \in W_2} - \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i.$$

(II) From the Lemma 7, if η is even then $-1 \in W_3$ and that $-W_j = \{-t : t \in W_j\} = W_{(j+3) \bmod 6}$, we get

$$S(\beta)(S(\beta) + 1) = -\frac{n-1}{4} - \frac{1}{2} - \frac{a-2x}{18} \left(\sum_{i \in W_0} - 2 \sum_{i \in W_1} + \sum_{i \in W_2} + \sum_{i \in W_3} - 2 \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i$$

$$+ \frac{b-2y}{6} \left(\sum_{i \in W_0} - \sum_{i \in W_2} + \sum_{i \in W_3} - \sum_{i \in W_5} \right) \beta^i,$$

$$T(\beta)(T(\beta) + 1) = -\frac{n-1}{4} - \frac{1}{2} - \frac{a-2x}{18} \left(\sum_{i \in W_0} + \sum_{i \in W_1} - 2 \sum_{i \in W_2} + \sum_{i \in W_3} + \sum_{i \in W_4} - 2 \sum_{i \in W_5} \right) \beta^i$$

$$+ \frac{b-2y}{6} \left(- \sum_{i \in W_0} + \sum_{i \in W_1} - \sum_{i \in W_3} + \sum_{i \in W_4} \right) \beta^i \text{ and}$$

$$U(\beta)(U(\beta) + 1) = -\frac{n-1}{4} - \frac{1}{2} - \frac{a-2x}{18} \left(-2 \sum_{i \in W_0} + \sum_{i \in W_1} + \sum_{i \in W_2} - 2 \sum_{i \in W_3} + \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i$$

$$+ \frac{b-2y}{6} \left(- \sum_{i \in W_1} + \sum_{i \in W_2} - \sum_{i \in W_4} + \sum_{i \in W_5} \right) \beta^i.$$

From Lemma 6, Table 1 and Table 2, we get the desired result.

□

We need to discuss the factorization of $x^n - 1$ over $\text{GF}(q)$. Let β be the same as before. Define for each i ; $0 \leq i \leq 5$,

$$\omega_i(x) = \prod_{j \in W_i} (x - \beta^j),$$

where W_i denote the Whiteman's cyclotomic classes of order 6. Among the n th roots of unity β^i , where $0 \leq i \leq n-1$, the n_2 elements $\beta^i, i \in P \cup \{0\}$, are n_2 th roots of unity, the n_1 elements $\beta^i, i \in Q \cup \{0\}$, are n_1 th roots of unity. Hence,

$$x^{n_2} - 1 = \prod_{i \in P \cup \{0\}} (x - \beta^i)$$

and

$$x^{n_1} - 1 = \prod_{i \in Q \cup \{0\}} (x - \beta^i).$$

Then, we have $x^n - 1 = \prod_{i=0}^{n-1} (x - \beta^i) = \frac{(x^{n_1}-1)(x^{n_2}-1)}{x-1} \omega(x)$, where $\omega(x) = \prod_{i=0}^5 \omega_i(x)$. It is straightforward to prove that if $q \in W_0$ then $\omega_i(x) \in \text{GF}(q)$ for all i .

Let $\Delta_1 = \frac{n_1+1}{2} \pmod{p}$, $\Delta_2 = \frac{n_2-1}{2} \pmod{p}$ and $\Delta = \frac{(n_1+1)(n_2-1)}{2} \pmod{p}$. From Corollary 1, we have the following theorems. First, we derive the expression of generator polynomial $g(x)$ for the case $q \notin W_0$.

Theorem 1. *Let the symbols be defined as before and assume that $q \notin W_0$. Then the generator polynomial $g(x)$ of the sequence s^∞ (defined in (5)) is expressed as*

$$g(x) = \begin{cases} x^n - 1, & \text{if } \Delta_1 \neq 0, \Delta_2 \neq 0, \Delta \neq 0 \\ \frac{x^n - 1}{x - 1}, & \text{if } \Delta_1 \neq 0, \Delta_2 \neq 0, \Delta = 0 \\ \frac{x^n - 1}{x^{n_2} - 1}, & \text{if } \Delta_1 = 0, \Delta_2 \neq 0 \\ \frac{x^n - 1}{x^{n_1} - 1}, & \text{if } \Delta_1 \neq 0, \Delta_2 = 0 \\ \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)}, & \text{if } \Delta_1 = \Delta_2 = 0. \end{cases}$$

The linear span of the sequence s^∞ is equal to $\deg(g(x))$. In this case, the cyclic code C_s over $\text{GF}(q)$ defined by the two-prime WGCS-II of order 6 (defined in (5)) has generator polynomial $g(x)$ as above and parameters $[n, k, d]$, where the dimension $k = n - \deg(g(x))$.

Proof. If $q \notin W_0$. Then, from Part I of Corollary 1, we have $S(\beta), T(\beta)$ and $U(\beta) \neq 0, -1$. Therefore, from Lemma 10, $S(\beta^t) = 0$ only when t is in P or Q or both. So, from (13) and Lemma 10 the generator polynomial of the cyclic code C_s defined by s^∞ is expressed as above. \square

The following theorem give the expression of the generator polynomials $g_i(x)$, $1 \leq i \leq 5$ for the case $q \in W_0$.

Theorem 2. *Let the symbols be defined as before. Let $q \in W_0$. Then we have the following results.*

(I) For $\Delta_1 \neq 0$, $\Delta_2 \neq 0$ and $\Delta \neq 0$, let $g_1(x)$ denote the generator polynomial of cyclic code generated by the two-prime WGCS-II with order 6 (defined in (5)). Then we have

$$g_1(x) = \left\{ \begin{array}{ll} x^n - 1 & \text{if } S(\beta) \neq 0, -1, T(\beta) \neq 0, -1, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_0(x)} & \text{if } S(\beta) = 0, T(\beta) \neq 0, -1, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_3(x)} & \text{if } S(\beta) = -1, T(\beta) \neq 0, -1, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_4(x)} & \text{if } T(\beta) = 0, S(\beta) \neq 0, -1, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_1(x)} & \text{if } T(\beta) = -1, S(\beta) \neq 0, -1, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_5(x)} & \text{if } U(\beta) = 0, S(\beta) \neq 0, -1, T(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_2(x)} & \text{if } U(\beta) = -1, S(\beta) \neq 0, -1, T(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_0(x)\omega_4(x)} & \text{if } S(\beta) = T(\beta) = 0, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_0(x)\omega_1(x)} & \text{if } S(\beta) = 0, T(\beta) = -1, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_3(x)\omega_4(x)} & \text{if } S(\beta) = -1, T(\beta) = 0, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_3(x)\omega_1(x)} & \text{if } S(\beta) = T(\beta) = -1, U(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_0(x)\omega_5(x)} & \text{if } S(\beta) = U(\beta) = 0, T(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_0(x)\omega_2(x)} & \text{if } S(\beta) = 0, U(\beta) = -1, T(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_3(x)\omega_5(x)} & \text{if } S(\beta) = -1, U(\beta) = 0, T(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_3(x)\omega_2(x)} & \text{if } S(\beta) = U(\beta) = -1, T(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_4(x)\omega_5(x)} & \text{if } T(\beta) = U(\beta) = 0, S(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_4(x)\omega_2(x)} & \text{if } T(\beta) = 0, U(\beta) = -1, S(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_1(x)\omega_5(x)} & \text{if } T(\beta) = -1, U(\beta) = 0, S(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_1(x)\omega_2(x)} & \text{if } T(\beta) = U(\beta) = -1, S(\beta) \neq 0, -1, \\ \frac{x^n - 1}{\omega_0(x)\omega_4(x)\omega_5(x)} & \text{if } S(\beta) = T(\beta) = U(\beta) = 0, \\ \frac{x^n - 1}{\omega_0(x)\omega_4(x)\omega_2(x)} & \text{if } S(\beta) = T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n - 1}{\omega_0(x)\omega_1(x)\omega_5(x)} & \text{if } S(\beta) = 0, T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n - 1}{\omega_0(x)\omega_1(x)\omega_2(x)} & \text{if } S(\beta) = 0, T(\beta) = U(\beta) = -1, \\ \frac{x^n - 1}{\omega_3(x)\omega_4(x)\omega_5(x)} & \text{if } S(\beta) = -1, T(\beta) = U(\beta) = 0, \\ \frac{x^n - 1}{\omega_3(x)\omega_4(x)\omega_2(x)} & \text{if } S(\beta) = -1, T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n - 1}{\omega_3(x)\omega_1(x)\omega_5(x)} & \text{if } S(\beta) = T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n - 1}{\omega_3(x)\omega_1(x)\omega_2(x)} & \text{if } S(\beta) = T(\beta) = U(\beta) = -1. \end{array} \right.$$

(II) For $\Delta_1 \neq 0$, $\Delta_2 \neq 0$ and $\Delta = 0$, let $g_2(x)$ denote the generator polynomial of cyclic code generated by the two-prime WGCS-II of order 6 (defined in (5)). And let $g_1(x)$ be the same as in (I). Then we have $g_2(x) = \frac{g_1(x)}{x-1}$.

(III) For $\triangle_1 \neq 0$ and $\triangle_2 = 0$, let $g_3(x)$ denote the generator polynomial of cyclic code generated by the two-prime WGCS-II of order 6 (defined in (5)). And let $g_1(x)$ be the same as in (I). Then we have

$$g_3(x) = \frac{g_1(x)}{x^{n_1}-1}.$$

(IV) For $\triangle_2 \neq 0$ and $\triangle_1 = 0$, let $g_4(x)$ denote the generator polynomial of cyclic code generated by the two-prime WGCS-II of order 6 (defined in (5)). And let $g_1(x)$ be the same as in (I). Then we have

$$g_4(x) = \frac{g_1(x)}{x^{n_2}-1}.$$

(V) For $\triangle_1 = \triangle_2 = 0$, let $g_5(x)$ denote the generator polynomial of cyclic code generated by the two-prime WGCS-II of order 6 (defined in (5)). And let $g_1(x)$ be the same as in (I). Then we have

$$g_5(x) = \frac{g_1(x)(x-1)}{(x^{n_1}-1)(x^{n_2}-1)}.$$

Proof. From Part II of Corollary 1, if $q \in W_0$ then we have $S(\beta), T(\beta), U(\beta) \in \text{GF}(q)$. Hence, it is possible that $S(\beta) \in \{0, -1\}$, $T(\beta) \in \{0, -1\}$, and $U(\beta) \in \{0, -1\}$. The conclusion on the generator polynomial $g_1(x)$ of cyclic code generated by the two-prime WGCS-II of order 6 follows from Theorem 1 and Lemma 10.

We give the following corollary for $S(\beta)(S(\beta)+1) = 0$, $T(\beta)(T(\beta)+1) = 0$ and $U(\beta)(U(\beta)+1) = 0$. \square

Corollary 2. *Let the symbols be defined as before. We have the following conclusions for $q \in W_0$.*

When $n \equiv 1 \pmod{12}$ and $\frac{n-1}{4} \equiv 0 \pmod{p}$ or $n \equiv 7 \pmod{12}$ and $\frac{n+1}{4} \equiv 0 \pmod{p}$ then the generator polynomial $g_1(x)$ (defined as above) is expressed as:

Case (I) If $\rho - \varrho \equiv 0 \pmod{3}$,

$$g_1(x) = \begin{cases} \frac{x^n-1}{\omega_0(x)\omega_4(x)\omega_5(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = U(\beta) = 0, \\ \frac{x^n-1}{\omega_0(x)\omega_4(x)\omega_2(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n-1}{\omega_0(x)\omega_1(x)\omega_5(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = 0, T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n-1}{\omega_0(x)\omega_1(x)\omega_2(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = 0, T(\beta) = U(\beta) = -1, \\ \frac{x^n-1}{\omega_3(x)\omega_4(x)\omega_5(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = -1, T(\beta) = U(\beta) = 0, \\ \frac{x^n-1}{\omega_3(x)\omega_4(x)\omega_2(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = -1, T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n-1}{\omega_3(x)\omega_1(x)\omega_5(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n-1}{\omega_3(x)\omega_1(x)\omega_2(x)}, & \text{if } \frac{2y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = U(\beta) = -1. \end{cases}$$

Case (II) If $\rho - \varrho \equiv 1 \pmod{3}$,

$$g_1(x) = \begin{cases} \frac{x^n-1}{\omega_0(x)\omega_4(x)\omega_5(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = U(\beta) = 0, \\ \frac{x^n-1}{\omega_0(x)\omega_4(x)\omega_2(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n-1}{\omega_0(x)\omega_1(x)\omega_5(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = 0, T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n-1}{\omega_0(x)\omega_1(x)\omega_2(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = 0, T(\beta) = U(\beta) = -1, \\ \frac{x^n-1}{\omega_3(x)\omega_4(x)\omega_5(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = -1, T(\beta) = U(\beta) = 0, \\ \frac{x^n-1}{\omega_3(x)\omega_4(x)\omega_2(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = -1, T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n-1}{\omega_3(x)\omega_1(x)\omega_5(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n-1}{\omega_3(x)\omega_1(x)\omega_2(x)}, & \text{if } \frac{x+y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = U(\beta) = -1. \end{cases}$$

Case (III) If $\rho - \varrho \equiv 2 \pmod{3}$,

$$g_1(x) = \begin{cases} \frac{x^n-1}{\omega_0(x)\omega_4(x)\omega_5(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = U(\beta) = 0, \\ \frac{x^n-1}{\omega_0(x)\omega_4(x)\omega_2(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n-1}{\omega_0(x)\omega_1(x)\omega_5(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = 0, T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n-1}{\omega_0(x)\omega_1(x)\omega_2(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = 0, T(\beta) = U(\beta) = -1, \\ \frac{x^n-1}{\omega_3(x)\omega_4(x)\omega_5(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = -1, T(\beta) = U(\beta) = 0, \\ \frac{x^n-1}{\omega_3(x)\omega_4(x)\omega_2(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = -1, T(\beta) = 0, U(\beta) = -1, \\ \frac{x^n-1}{\omega_3(x)\omega_1(x)\omega_5(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = -1, U(\beta) = 0, \\ \frac{x^n-1}{\omega_3(x)\omega_1(x)\omega_2(x)}, & \text{if } \frac{x-y}{3} \equiv 0 \pmod{p} \text{ and } S(\beta) = T(\beta) = U(\beta) = -1. \end{cases}$$

For $j = 2, 3, 4, 5$, the generator polynomials $g_j(x)$ (defined as in Theorem 2) can be expressed in a similar fashion as above (as for $g_1(x)$) for η is even and odd.

Proof. From Lemma 4, if η is odd then $n \equiv 1 \pmod{12}$. Let $n \equiv 1 \pmod{12}$ and $(n-1)/4 \equiv 0 \pmod{p}$.

By Lemma 6, we have

$$\begin{aligned} & \text{if } \rho - \varrho \equiv 0 \pmod{3}, \text{ then } (2y)/3 \text{ is an integer,} \\ & \text{if } \rho - \varrho \equiv 1 \pmod{3}, \text{ then } (x+y)/3 \text{ is an integer and} \\ & \text{if } \rho - \varrho \equiv 2 \pmod{3}, \text{ then } (x-y)/3 \text{ is an integer.} \end{aligned}$$

By the help of Lemma 11 and Theorem 2, we get the desired result on the generator polynomial $g_1(x)$ of cyclic code generated by two-prime WGCS-II with order 6. In this case, the cyclic code C_s over $\text{GF}(q)$ defined by sequence s^∞ has parameters $[n, k, d]$, where the dimension $k = n - \deg(g_1(x))$. In a similar fashion, we get the result for $n \equiv 7 \pmod{12}$ and $\frac{n+1}{4} \equiv 0 \pmod{p}$. \square

Remark. We discuss the cases for $\frac{2y}{3} \pmod{p} \neq 0$, $\frac{x+y}{3} \pmod{p} \neq 0$ and $\frac{x-y}{3} \pmod{p} \neq 0$ in

the above corollary. Let $C_0 = \left(\sum_{i \in W_0} + \sum_{i \in W_3} \right) \beta^i$, $C_1 = \left(\sum_{i \in W_1} + \sum_{i \in W_4} \right) \beta^i$ and $C_2 = \left(\sum_{i \in W_2} + \sum_{i \in W_5} \right) \beta^i$.

When $n \equiv 1 \pmod{12}$ and $\frac{n-1}{4} \equiv 0 \pmod{p}$ or $n \equiv 7 \pmod{12}$ and $\frac{n+1}{4} \equiv 0 \pmod{p}$. We have following three cases:

(I) If $\rho - \varrho \equiv 0 \pmod{3}$ and $\frac{2y}{3} \pmod{p} \neq 0$, (II) $\rho - \varrho \equiv 1 \pmod{3}$ and $\frac{x+y}{3} \pmod{p} \neq 0$ and (III) $\rho - \varrho \equiv 2 \pmod{3}$ and $\frac{x-y}{3} \pmod{p} \neq 0$.

(I) If $\rho - \varrho \equiv 0 \pmod{3}$ and $\frac{2y}{3} \pmod{p} \neq 0$, then we have

$$\begin{aligned}
S(\beta)(S(\beta) + 1) &= 0 & \text{if } C_2 - C_0 = 0, C_0 - C_1 \neq 0, C_1 - C_2 \neq 0, \\
T(\beta)(T(\beta) + 1) &= 0 & \text{if } C_0 - C_1 = 0, C_2 - C_0 \neq 0, C_1 - C_2 \neq 0, \\
U(\beta)(U(\beta) + 1) &= 0 & \text{if } C_1 - C_2 = 0, C_2 - C_0 \neq 0, C_0 - C_1 \neq 0, \\
S(\beta)(S(\beta) + 1) = 0 \text{ and } T(\beta)(T(\beta) + 1) = 0 & \text{if } C_2 - C_0 = 0, C_0 - C_1 = 0, C_1 - C_2 \neq 0, \\
S(\beta)(S(\beta) + 1) = 0 \text{ and } U(\beta)(U(\beta) + 1) = 0 & \text{if } C_2 - C_0 = 0, C_1 - C_2 = 0, C_0 - C_1 \neq 0, \\
T(\beta)(T(\beta) + 1) = 0 \text{ and } U(\beta)(U(\beta) + 1) = 0 & \text{if } C_0 - C_1 = 0, C_1 - C_2 = 0, C_2 - C_0 \neq 0, \\
S(\beta)(S(\beta) + 1) = 0, T(\beta)(T(\beta) + 1) = 0 & \text{if } C_2 - C_0 = 0, C_0 - C_1 = 0, C_1 - C_2 = 0. \\
\text{and } U(\beta)(U(\beta) + 1) = 0
\end{aligned}$$

From the above expressions, we get the similar result on generator polynomials as in Theorem 2 with condition on $S(\beta)$, $U(\beta)$, $T(\beta)$, $C_0 - C_1$, $C_1 - C_2$ and $C_2 - C_0$. Similarly, we get the condition for $\rho - \varrho \equiv 1 \pmod{3}$ and $\frac{x+y}{3} \pmod{p} \neq 0$ and for $\rho - \varrho \equiv 2 \pmod{3}$ and $\frac{x-y}{3} \pmod{p} \neq 0$.

4. THE MINIMUM DISTANCE OF THE CYCLIC CODES

In this section, we determine the lower bounds on the minimum distance of some of the cyclic codes of this paper.

Theorem 3. [5] Let C_i denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g_i(x) = \frac{x^n - 1}{x^{n_i} - 1}$. The cyclic code C_i has parameters $[n, n_i, d_i]$, where $d_i = n_{i-(-1)^i}$ and $i = 1, 2$.

Theorem 4. [5] Let $C_{(n_1, n_2, q)}$ denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)}$. The cyclic code $C_{(n_1, n_2, q)}$ has parameters $[n, n_1 + n_2 - 1, d_{(n_1, n_2, q)}]$, where $d_{(n_1, n_2, q)} = \min(n_1, n_2)$.

Theorem 5. Assume that $q \in W_0$. Let $C_{(n_i, q)}^{(i, j)}$ denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g_{(n_i, q)}^{(i, j)}(x) = \frac{x^n - 1}{(x^{n_i} - 1)\omega_j(x)}$, where $i = 1, 2$, and $0 \leq j \leq 5$. The cyclic code $C_{(n_i, q)}^{(i, j)}$ has parameters $[n, n_i + \frac{(n_1 - 1)(n_2 - 1)}{6}, d_{(n_i, q)}^{(i, j)}]$, where $d_{(n_i, q)}^{(i, j)} \geq \lceil \sqrt{n_{i-(-1)^i}} \rceil$. If $-1 \in W_3$, we have $(d_{(n_i, q)}^{(i, j)})^2 - d_{(n_i, q)}^{(i, j)} + 1 \geq n_{i-(-1)^i}$.

Proof. Let $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, j)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. Then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, (j-k) \bmod 6)}$. It then follows that $d_{(n_i, q)}^{(i, j)} = d_{(n_i, q)}^{(i, (j-k) \bmod 6)}$. Therefore, we have $d_{(n_i, q)}^{(i, 0)} = d_{(n_i, q)}^{(i, 1)} = d_{(n_i, q)}^{(i, 2)} = d_{(n_i, q)}^{(i, 3)} = d_{(n_i, q)}^{(i, 4)} = d_{(n_i, q)}^{(i, 5)}$. Let $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of minimum weight in $C_{(n_i, q)}^{(i, j)}$. Then $c(x^r)$ is a codeword of same weight in $C_{(n_i, q)}^{(i, (j-k) \bmod 6)}$. Further, for any $r \in W_k$, we have $c(x)c(x^r)$ is a codeword of C_i , where C_i denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g_i(x) = \frac{x^n - 1}{x^{n_i} - 1}$ and minimum distance $d_i = n_{i-(-1)^i}$. Hence, from Theorem 3, we have $(d_{(n_i, q)}^{(i, j)})^2 \geq d_i = n_{i-(-1)^i}$, and $(d_{(n_i, q)}^{(i, j)})^2 - d_{(n_i, q)}^{(i, j)} + 1 \geq n_{i-(-1)^i}$ if $-1 \in W_3$. \square

Theorem 6. Assume that $q \in W_0$. Let $C_{(n_1, n_2, q)}^{(j)}$ denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g_{(n_1, n_2, q)}^{(j)}(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)\omega_j(x)}$, where $0 \leq j \leq 5$. The cyclic code $C_{(n_1, n_2, q)}^{(j)}$ has parameters $[n, n_1 + n_2 - 1 + \frac{(n_1 - 1)(n_2 - 1)}{6}, d_{(n_1, n_2, q)}^{(j)}]$, where $d_{(n_1, n_2, q)}^{(j)} \geq \lceil \sqrt{\min(n_1, n_2)} \rceil$. If $-1 \in W_3$, we have $(d_{(n_1, n_2, q)}^{(j)})^2 - d_{(n_1, n_2, q)}^{(j)} + 1 \geq \min(n_1, n_2)$.

Proof. Let $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{(j)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. Then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{((j-k) \bmod 6)}$. It then follows that $d_{(n_1, n_2, q)}^{(j)} = d_{(n_1, n_2, q)}^{((j-k) \bmod 6)}$. Therefore, we have $d_{(n_1, n_2, q)}^{(0)} = d_{(n_1, n_2, q)}^{(1)} = d_{(n_1, n_2, q)}^{(2)} = d_{(n_1, n_2, q)}^{(3)} = d_{(n_1, n_2, q)}^{(4)} = d_{(n_1, n_2, q)}^{(5)}$. Let $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of minimum weight in $C_{(n_1, n_2, q)}^{(j)}$. Then $c(x^r)$ is a codeword of same weight in $C_{(n_1, n_2, q)}^{((j-k) \bmod 6)}$. Further, for any $r \in W_k$, we have $c(x)c(x^r)$ is a codeword of $C_{(n_1, n_2, q)}$, where $C_{(n_1, n_2, q)}$ denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)}$ and minimum distance $d_{(n_1, n_2, q)} = \min(n_1, n_2)$. Hence, from Theorem 4, we have $(d_{(n_1, n_2, q)}^{(j)})^2 \geq d_{(n_1, n_2, q)} = \min(n_1, n_2)$, and $(d_{(n_1, n_2, q)}^{(j)})^2 - d_{(n_1, n_2, q)}^{(j)} + 1 \geq \min(n_1, n_2)$ if $-1 \in W_3$. \square

Theorem 7. Assume that $q \in W_0$. Let $C_{(n_i, q)}^{(i, j, h)}$ denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g_{(n_i, q)}^{(i, j, h)}(x) = \frac{x^n - 1}{(x^{n_i} - 1)\omega_j(x)\omega_h(x)}$, where $i = 1, 2$ and $(j, h) \in \{(0, 1), (0, 2), (1, 2), (1, 3), (2, 3), (2, 4), (3, 4), (3, 5), (4, 0), (4, 5), (5, 0), (5, 1)\}$. The cyclic code $C_{(n_i, q)}^{(i, j, h)}$ has parameters $[n, n_i + \frac{(n_1 - 1)(n_2 - 1)}{3}, d_{(n_i, q)}^{(i, j, h)}]$, where $d_{(n_i, q)}^{(i, j, h)} \geq \lceil \sqrt{n_{i-(-1)^i}} \rceil$. If $-1 \in W_3$, we have $(d_{(n_i, q)}^{(i, j, h)})^2 - d_{(n_i, q)}^{(i, j, h)} + 1 \geq n_{i-(-1)^i}$.

Proof. Let $j = 0, h = 1$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, 0, 1)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. Then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, (0-k) \bmod 6, (1-k) \bmod 6)}$. It then follows that $d_{(n_i, q)}^{(i, 0, 1)} = d_{(n_i, q)}^{(i, (0-k) \bmod 6, (1-k) \bmod 6)}$. Therefore, we have

$$d_{(n_i, q)}^{(i, 0, 1)} = d_{(n_i, q)}^{(i, 5, 0)} = d_{(n_i, q)}^{(i, 4, 5)} = d_{(n_i, q)}^{(i, 3, 4)} = d_{(n_i, q)}^{(i, 2, 3)} = d_{(n_i, q)}^{(i, 1, 2)}. \quad (22)$$

Let $j = 0, h = 2$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, 0, 2)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. Then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, (0-k) \bmod 6, (2-k) \bmod 6)}$. It then follows that $d_{(n_i, q)}^{(i, 0)} = d_{(n_i, q)}^{(i, (0-k) \bmod 6, (2-k) \bmod 6)}$. Therefore, we have

$$d_{(n_i, q)}^{(i, 0, 2)} = d_{(n_i, q)}^{(i, 5, 1)} = d_{(n_i, q)}^{(i, 4, 0)} = d_{(n_i, q)}^{(i, 3, 5)} = d_{(n_i, q)}^{(i, 2, 4)} = d_{(n_i, q)}^{(i, 1, 3)}. \quad (23)$$

Further, from (22) and (23) for any $r \in W_3$, we have that $c(x)c(x^r)$ is a codeword of C_i . where C_i denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g_i(x) = \frac{x^n - 1}{x^{n_i} - 1}$ and minimum distance $d_i = n_{i-(-1)^i}$. Hence, from Theorem 3, we have $(d_{(n_i, q)}^{i, j, h})^2 \geq d_i = n_{i-(-1)^i}$, i.e., $d_{(n_i, q)}^{(i, j, h)} \geq \lceil \sqrt{n_{i-(-1)^i}} \rceil$ and $(d_{(n_i, q)}^{(i, j, h)})^2 - d_{(n_i, q)}^{(i, j, h)} + 1 \geq n_{i-(-1)^i}$ if $-1 \in W_3$. \square

Theorem 8. Assume that $q \in W_0$. Let $C_{(n_1, n_2, q)}^{(j, h)}$ denote the cyclic code over $\text{GF}(q)$ with the generator polynomial $g_{(n_1, n_2, q)}^{(j, h)}(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)\omega_j(x)\omega_h(x)}$, where $(j, h) \in \{(0, 1), (0, 2), (1, 2), (1, 3), (2, 3), (2, 4), (3, 4), (3, 5), (4, 0), (4, 5), (5, 0), (5, 1)\}$. The cyclic code $C_{(n_1, n_2, q)}^{(j, h)}$ has parameters $[n, n_1 + n_2 - 1 + \frac{(n_1 - 1)(n_2 - 1)}{3}, d_{(n_1, n_2, q)}^{(j, h)}]$, where $d_{(n_1, n_2, q)}^{(j, h)} \geq \lceil \sqrt{\min(n_1, n_2)} \rceil$. If $-1 \in W_3$, we have $(d_{(n_1, n_2, q)}^{(j, h)})^2 - d_{(n_1, n_2, q)}^{(j, h)} + 1 \geq \min(n_1, n_2)$.

Proof. Let $j = 0, h = 1$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{(0, 1)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{(i, (0-k) \bmod 6, (1-k) \bmod 6)}$. It then follows that $d_{(n_1, n_2, q)}^{(0, 1)} = d_{(n_1, n_2, q)}^{((0-k) \bmod 6, ((1-k) \bmod 6)}$. Therefore, we have

$$d_{(n_1, n_2, q)}^{(0, 1)} = d_{(n_1, n_2, q)}^{(5, 3)} = d_{(n_1, n_2, q)}^{(4, 5)} = d_{(n_1, n_2, q)}^{(3, 4)} = d_{(n_1, n_2, q)}^{(2, 3)} = d_{(n_1, n_2, q)}^{(1, 2)}. \quad (24)$$

Let $j = 0, h = 2$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{(0, 2)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$, then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{((0-k) \bmod 6, (2-k) \bmod 6)}$.

It then follows that $d_{(n_1, n_2, q)}^{(0,2)} = d_{(n_1, n_2, q)}^{((0-k) \bmod 6, (2-k) \bmod 6)}$. Therefore, we have

$$d_{(n_1, n_2, q)}^{(0,2)} = d_{(n_1, n_2, q)}^{(5,1)} = d_{(n_1, n_2, q)}^{(4,0)} = d_{(n_1, n_2, q)}^{(3,5)} = d_{(n_1, n_2, q)}^{(2,4)} = d_{(n_1, n_2, q)}^{(1,3)}. \quad (25)$$

Further, from (24) and (25) for any $r \in W_3$, we have that $c(x)c(x^r)$ is a codeword of C_i . Hence, from Theorem 4, we have $(d_{(n_1, n_2, q)}^{(j,h)})^2 \geq d_{(n_1, n_2, q)} = \min(n_1, n_2)$ i.e., $d_{(n_1, n_2, q)}^{(j,h)} \geq \lceil \sqrt{\min(n_1, n_2)} \rceil$, and $(d_{(n_1, n_2, q)}^{(j,h)})^2 - d_{(n_1, n_2, q)}^{(j,h)} + 1 \geq \min(n_1, n_2)$ if $-1 \in W_3$. \square

Theorem 9. Assume that $q \in W_0$. Let $C_{(n_i, q)}^{(i, j, h, l)}$ denote the cyclic code over $\text{GF}(q)$ with the generator

polynomial $g_{(n_i, q)}^{(i, j, h, l)}(x) = \frac{x^n - 1}{(x^{n_i} - 1)\omega_j(x)\omega_h(x)\omega_l(x)}$, where $i = 1, 2$ and

$(j, h, l) \in \{(0, 4, 2), (0, 4, 5), (1, 5, 0), (2, 0, 1), (3, 1, 2), (4, 2, 3), (5, 3, 1), (5, 3, 4)\}$.

The cyclic code $C_{(n_i, q)}^{(i, j, h, l)}$ has parameters $[n, n_i + \frac{(n_1 - 1)(n_2 - 1)}{2}, d_{(n_i, q)}^{(i, j, h, l)}]$, where $d_{(n_i, q)}^{(i, j, h, l)} \geq \lceil \sqrt{n_i - (-1)^i} \rceil$.

If $-1 \in W_3$, we have $(d_{(n_1, n_2, q)}^{(j, h, l)})^2 - d_{(n_1, n_2, q)}^{(j, h, l)} + 1 \geq n_i - (-1)^i$.

Proof. Let $j = 0, h = 4, l = 2$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, 0, 4, 2)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. The cyclic code $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, (0-k) \bmod 6, (4-k) \bmod 6, (2-k) \bmod 6)}$. It then follows that

$d_{(n_i, q)}^{(i, 0, 4, 2)} = d_{(n_i, q)}^{(i, (0-k) \bmod 6, (4-k) \bmod 6, (2-k) \bmod 6)}$. Therefore, we have

$$d_{(n_i, q)}^{(i, 0, 4, 2)} = d_{(n_i, q)}^{(i, 5, 3, 1)} = d_{(n_i, q)}^{(i, 4, 2, 0)} = d_{(n_i, q)}^{(i, 3, 1, 5)} = d_{(n_i, q)}^{(i, 2, 0, 4)} = d_{(n_i, q)}^{(i, 1, 5, 3)}. \quad (26)$$

Let $j = 0, h = 4, l = 5$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, 0, 4, 5)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. Then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_i, q)}^{(i, (0-k) \bmod 6, (4-k) \bmod 6, (5-k) \bmod 6)}$. It then follows that

$d_{(n_i, q)}^{(i, 0, 4, 5)} = d_{(n_i, q)}^{(i, (0-k) \bmod 6, (4-k) \bmod 6, (5-k) \bmod 6)}$. Therefore, we have

$$d_{(n_i, q)}^{(i, 0, 4, 5)} = d_{(n_i, q)}^{(i, 5, 3, 4)} = d_{(n_i, q)}^{(i, 4, 2, 3)} = d_{(n_i, q)}^{(i, 3, 1, 2)} = d_{(n_i, q)}^{(i, 2, 0, 1)} = d_{(n_i, q)}^{(i, 1, 5, 0)}. \quad (27)$$

Further, from (26) and (27) for any $r \in W_3$, we have that $c(x)c(x^r)$ is a codeword of C_i , where C_i and d_i be defined as in Theorem 3. Hence, from Theorem 3, we have $(d_{(n_i, q)}^{(i, j, h, l)})^2 \geq d_i = n_i - (-1)^i$, i.e., $d_{(n_i, q)}^{(i, j, h, l)} \geq \lceil \sqrt{n_i - (-1)^i} \rceil$ and $(d_{(n_i, q)}^{(i, j, h, l)})^2 - d_{(n_i, q)}^{(i, j, h, l)} + 1 \geq n_i - (-1)^i$, if $-1 \in W_3$. \square

Theorem 10. Assume that $q \in W_0$. Let $C_{(n_1, n_2, q)}^{(j, h, l)}$ denote the cyclic code over $\text{GF}(q)$ with the generator

polynomial $g_{(n_1, n_2, q)}^{(j, h, l)}(x) = \frac{(x^n - 1)(x - 1)}{(x^{n_1} - 1)(x^{n_2} - 1)\omega_j(x)\omega_h(x)\omega_l(x)}$, where

$(j, h, l) \in \{(0, 4, 2), (0, 4, 5), (1, 5, 0), (2, 0, 1), (3, 1, 2), (4, 2, 3), (5, 3, 1), (5, 3, 4)\}$. The cyclic code $C_{(n_1, n_2, q)}^{(j, h, l)}$ has parameters $[n, n_1 + n_2 - 1 + \frac{(n_1-1)(n_2-1)}{2}, d_{(n_1, n_2, q)}^{(j, h, l)}]$, where $d_{(n_1, n_2, q)}^{(j, h, l)} \geq \lceil \sqrt{\min(n_1, n_2)} \rceil$. If $-1 \in W_3$, we have $(d_{(n_1, n_2, q)}^{(j, h, l)})^2 - d_{(n_1, n-2, q)}^{(j, h, l)} + 1 \geq \min(n_1, n_2)$.

Proof. Let $j = 0, h = 4, l = 2$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{(0, 4, 2)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. Then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{((0-k) \bmod 6, (4-k) \bmod 6, (2-k) \bmod 6)}$. It then follows that $d_{(n_1, n_2, q)}^{(i, 0, 4, 2)} = d_{(n_1, n_2, q)}^{(i, (0-k) \bmod 6, (4-k) \bmod 6, (2-k) \bmod 6)}$. Therefore, we have

$$d_{(n_1, n_2, q)}^{(0, 4, 2)} = d_{(n_1, n_2, q)}^{(5, 3, 1)} = d_{(n_1, n_2, q)}^{(4, 2, 0)} = d_{(n_1, n_2, q)}^{(3, 1, 5)} = d_{(n_1, n_2, q)}^{(2, 0, 4)} = d_{(n_1, n_2, q)}^{(1, 5, 3)}. \quad (28)$$

Let $j = 0, h = 4, l = 5$ and $c(x) \in \text{GF}(q)[x]/(x^n - 1)$ be a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{(0, 4, 5)}$. Take any $r \in W_k$ for $1 \leq k \leq 5$. Then $c(x^r)$ is a codeword of Hamming weight ω in $C_{(n_1, n_2, q)}^{((0-k) \bmod 6, (4-k) \bmod 6, (5-k) \bmod 6)}$. It then follows that $d_{(n_1, n_2, q)}^{(i, 0, 4, 5)} = d_{(n_1, n_2, q)}^{(i, (0-k) \bmod 6, (4-k) \bmod 6, (5-k) \bmod 6)}$. Therefore, we have

$$d_{(n_1, n_2, q)}^{(0, 4, 5)} = d_{(n_1, n_2, q)}^{(5, 3, 4)} = d_{(n_1, n_2, q)}^{(4, 2, 3)} = d_{(n_1, n_2, q)}^{(3, 1, 2)} = d_{(n_1, n_2, q)}^{(2, 0, 1)} = d_{(n_1, n_2, q)}^{(1, 5, 3)}. \quad (29)$$

Further, from (28) and (29) for any $r \in W_3$, we have that $c(x)c(x^r)$ is a codeword of $C_{(n_1, n_2, q)}$, where $C_{(n_1, n_2, q)}$ and $d_{(n_1, n_2, q)}$ be defined as in Theorem 4. Hence, from Theorem 4, we have $(d_{(n_1, n_2, q)}^{(j, h, l)})^2 \geq d_{(n_1, n_2, q)} = \min(n_1, n_2)$, i.e., $d_{(n_1, n_2, q)}^{(j, h, l)} \geq \lceil \sqrt{\min(n_1, n_2)} \rceil$ and $(d_{(n_1, n_2, q)}^{(j, h, l)})^2 - d_{(n_1, n-2, q)}^{(j, h, l)} + 1 \geq \min(n_1, n_2)$ if $-1 \in W_3$. \square

Example 1. Let $(p, m, n_1, n_2) = (2, 1, 13, 19)$. Then $q = 2$, $n = 247$ and C_s is a $[247, 109]$ cyclic code over $\text{GF}(q)$ with generator polynomial $g(x) = \frac{x^{247}-1}{(x-1)\omega_0(x)\omega_1(x)\omega_2(x)} = x^{138} + x^{137} + x^{136} + x^{134} + x^{130} + x^{129} + x^{128} + x^{124} + x^{121} + x^{120} + x^{111} + x^{107} + x^{106} + x^{105} + x^{104} + x^{102} + x^{98} + x^{96} + x^{94} + x^{93} + x^{92} + x^{88} + x^{87} + x^{86} + x^{85} + x^{83} + x^{82} + x^{75} + x^{70} + x^{67} + x^{63} + x^{62} + x^{61} + x^{60} + x^{57} + x^{55} + x^{53} + x^{52} + x^{51} + x^{50} + x^{47} + x^{46} + x^{45} + x^{43} + x^{42} + x^{40} + x^{39} + x^{38} + x^{37} + x^{36} + x^{35} + x^{34} + x^{33} + x^{31} + x^{30} + x^{28} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{16} + x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^6 + x^3 + x^2 + 1$. We did some computation and our computation shows that upper bound on the minimum distance for this binary code is 48.

Example 2. Let $(p, m, n_1, n_2) = (3, 1, 7, 13)$. Then $q = 2$, $n = 91$ and C_s is a $[91, 19, 7]$ cyclic code over $\text{GF}(q)$ with generator polynomial $g(x) = \frac{(x^{91}-1)(x-1)}{(x^7-1)(x^{13}-1)} = x^{72} + x^{71} + x^{65} + x^{64} + x^{59} + x^{57} + x^{52} +$

$x^{50} + x^{46} + x^{43} + x^{39} + x^{36} + x^{33} + x^{29} + x^{26} + x^{22} + x^{20} + x^{15} + x^{13} + x^8 + x^7 + x + 1$. This is a bad cyclic code due to its poor minimum distance. The code in this case is bad because $q \notin W_0$.

Example 3. Let $(p, m, n_1, n_2) = (3, 1, 7, 19)$. Then $q = 3$, $n = 133$ and C_s is a $[133, 61]$ cyclic code over $\text{GF}(q)$ with generator polynomial $g(x) = \frac{x^{133}-1}{(x^7-1)\omega_3(x)\omega_4(x)\omega_2(x)} = x^{72} + 2x^{66} + x^{65} + 2x^{64} + 2x^{63} + 2x^{61} + x^{60} + 2x^{58} + 2x^{57} + 2x^{56} + x^{55} + x^{54} + x^{53} + 2x^{52} + x^{50} + 2x^{49} + x^{48} + 2x^{47} + 2x^{46} + 2x^{45} + x^{44} + 2x^{41} + x^{40} + x^{37} + 2x^{36} + x^{35} + x^{32} + 2x^{31} + x^{28} + 2x^{27} + 2x^{26} + 2x^{25} + x^{24} + 2x^{23} + x^{22} + 2x^{20} + x^{19} + x^{18} + x^{17} + 2x^{16} + 2x^{15} + 2x^{14} + x^{12} + 2x^{11} + 2x^9 + 2x^8 + x^7 + 2x^6 + 1$. We did some computation and our computation shows that upper bound on the minimum distance for this ternary code is 35. From Theorem 9, we have lower bound on the minimum distance for this ternary code is 5.

Conclusion. WGCS were used to construct cyclic codes in [5] and [12]. The idea of constructing cyclic codes with two-prime WGCS-II of order 6 could be viewed as an extension of above these two papers. The cyclic codes employed in this paper depend on n_1, n_2 and q . When $q \in W_0$, we get a good code. We expect that the codes in Examples 1 and 3 give good codes. When $q \notin W_0$, we get a bad code, for example, we get a bad code in Example 2. Finally, we expect that cyclic codes described in this paper can be employed to construct the good cyclic codes of large length.

REFERENCES

- [1] E. Betti and M. Sala. A new bound for the minimum distance of a cyclic code from its defining set. *IEEE Transactions on Information Theory*, 52(8):3700–3706, 2006.
- [2] Z. Chen and S. Li. Some notes on generalized cyclotomic sequences of length pq . *Journal of Computer Science and Technology*, 23:843–850, 2008.
- [3] T. Cusik, C. Ding, and A. Renvall. *Stream Ciphers and Number Theory*. North-Holland Mathematical Lib., North-Holland, 2003.
- [4] C. Ding. Linear complexity of generalized cyclotomic binary sequences of order 2. *Finite Fields Appl.*, 3(2):159–174, Apr. 1997.
- [5] C. Ding. Cyclic codes from the two-prime sequences. *IEEE Transactions on Information Theory*, 58(6):3881–3891, 2012.
- [6] C. Ding, X. Du, and Z. Zhou. The bose and minimum distance of a class of BCH codes. *IEEE Transactions on Information Theory*, 61(5):2351–2356, 2015.
- [7] M. Eupen and J. van Lint. On the minimum distance of ternary cyclic codes. *IEEE Transactions on Information Theory*, 39(2):409–416, 1993.
- [8] X. Gong, B. Zhang, D. Feng, and T. Yan. Autocorrelation values of new generalized cyclotomic sequences of order six over \mathbb{Z}_{pq} . *Information Security and Cryptology - 9th International Conference, Inscrypt 2013*, 86–98, 2013.
- [9] S. Li and T. Yan. Linear complexity of binary sextic whiteman generalized cyclotomic sequences. *Computer Engineering*, 36(4):150–154, 2010.
- [10] R. Lidl and H. Niederreiter. *Finite fields*. Cambridge Univ. Press, 1997.

- [11] F. Macwilliams and N. Sloane. The theory of error correcting codes. *North-Holland Mathematical Lib., North-Holland*, 1977.
- [12] Y. Sun, T. Yan, and H. Li. Cyclic code from the first class whiteman's generalized cyclotomic sequence with order 4. *CoRR*, abs/1303.6378, 2013.
- [13] J. van Lint and R. Wilson. On the minimum distance of cyclic codes. *IEEE Transactions on Information Theory*, 32(1):23–40, 1986.
- [14] A. L. Whiteman. A family of difference sets. *Illinois J. Math.*, 6:107–121, 1962.
- [15] C. Zhao, W. Ma, T. Yan, and Y. Sun. Autocorrelation values of generalized cyclotomic sequences of order six. *IEICE Transactions*, 96-A(10):2045–2048, 2013.

DEPARTMENT OF APPLIED MATHEMATICS, INDIAN SCHOOL OF MINES, DHANBAD 826 004, INDIA

E-mail address: kewat.pk.am@ismdhanbad.ac.in, priti.jsr13@gmail.com